https://www.elektroniknet.de/elektronik/embedded/wir-wollen-angreifern-stets-eine-nasenlaenge-voraus-sein-176762.html

world of solutions
Elektronik

Embedded-Security

»Wir wollen Angreifern stets eine Nasenlänge voraus sein«

25.05.2020Tobias Schlichtmeier

Mit der Vernetzung im IoT gewinnt das Thema Sicherheit zunehmend an Bedeutung. Ebenso sind Embedded-Systeme mit ausreichendem Schutz vor Hacker-Angriffen zu versehen. Wie das gelingt, erklärt Oliver Winzenried, CEO und Mitgründer von Wibu-Systems, im Elektronik-Interview.

Herr Winzenried, Wibu-Systems feierte letztes Jahr sein 30-jähriges Firmenjubiläum. Wie hat sich Ihr Unternehmen seit der Gründung weiterentwickelt?

Oliver Winzenried: Seit der Gründung im Jahr 1989 haben wir unsere Schutzanwendungen kontinuierlich erweitert, sodass wir inzwischen als weltweit anerkannter Technologieexperte gelten und zu den Top 3 der Anbieter von Softwarelizenzierungslösungen nach Marktanteilen gehören. Auch die Mitarbeiterzahl ist gewachsen. In der Firmenzentrale und den Tochtergesellschaften sind aktuell etwa 130 Mitarbeiter beschäftigt. Im Jahr 2021 ziehen wir in unseren Neubau mit größerer Bürofläche für weiteres Wachstum.

Bereits während des Studiums hatten Marcellus Buchheit und ich die Idee, einen sicheren und praxistauglichen Kopierschutz-Dongle für PC-Software zu entwickeln, denn damals gab es unseres Erachtens keine zuverlässige Anwendung. Unser erstes Produkt, die WibuBox für die parallele Schnittstelle, nutzte konsequent kryptografische Verfahren und bot ein höheres Sicherheitsniveau als Anwendungen der Mitbewerber.

https://www.elektroniknet.de/elektronik/embedded/wir-wollen-angreifern-stets-eine-nasenlaenge-voraus-sein-176762.html

Heute bieten wir nicht nur »Protection«, also Kopier- und Know-how-Schutz, sondern ebenfalls »Licensing« und »Security«, um den Herstellern flexible Lizenzmodelle und den Schutz vor Manipulation zu ermöglichen.

CodeMeter von Wibu-Systems schützt auch Embedded-Systeme. Können Sie erklären, wie CodeMeter arbeitet?
Winzenried: Schutz, Lizenzierung und Security basieren auf Verschlüsselung und Signaturen – egal, ob im Embedded- oder klassischen Softwarebereich. Allerdings können im Embedded-Bereich extremere Umweltbedingungen herrschen als im Büroalltag. Für diese Fälle haben wir spezielle Dongle-Varianten, die in heißen, kalten, feuchten und staubigen Umgebungen funktionieren.

Für PC-Software gibt es CodeMeter Runtime, ein fertiges Paket mit allen nötigen Komponenten als Schnittstelle zwischen geschützter Software und »Lizenz«. Das schlankere CodeMeter Embedded ist speziell für Embedded-Systeme ausgelegt und bietet eine Bibliothek, die kryptografische Funktionen und Funktionen zur Lizenzierung für Systeme wie Embedded Linux, VxWorks, QNX und Android zur Verfügung stellt. »CodeMeter µEmbedded« ist die CodeMeter-Variante, die speziell für Field Programmable Gate Arrays (FPGAs) und Mikrocontroller entwickelt wurde. Sie zeichnet sich durch einen extrem kleinen Speicherplatzbedarf von weniger als 60 Kilobyte für den Code aus. Alle Varianten sind kompatibel, was Lizenzen, Verteilung und Integration in Geschäftsprozesse beim Hersteller betrifft.

Grundsteinlegung der neuen Firmenzentrale von Wibu-Systems mit Dr. Frank Mentrup, Bastian Wieland, Oliver Winzenried, Prof. Dr. Jörn Müller-Quade und Hans Bosse (Wolff+Müller) (v.l.n.r.).

Unterstützt CodeMeter ebenfalls den Schutz von Software?
Winzenried: Mit dem Schutz von PC-Software mit WibuKey haben wir vor über dreißig Jahren begonnen. Heute ist Software nicht allein in PCs, sondern in allen möglichen Geräten, wie industriellen Kameras oder Computerradiographiegeräten in der Medizin im Einsatz. CodeMeter bietet einen plattformübergreifenden Schutz – egal, ob Hersteller ihre PC-, Embedded- oder Mikrocontroller-Software schützen wollen. Mithilfe unserer Technik verschlüsselt der Hersteller seine Software. Seine Kunden erhalten beim Kauf die geschützte Software und die Nutzungsrechte, die als Schlüssel in der

Schutzhardware »CmDongle«, der Aktivierungsdatei »CmActLicense« oder im »CmCloudContainer« in der Cloud sicher gespeichert werden. Genutzt wird diese »Lizenz« lokal oder über das Netzwerk. Kauft der Anwender zu einem späteren Zeitpunkt weitere Funktionen der Software, so kann der Hersteller aus der Ferne die Lizenz aktualisieren.

»Wir sehen Cloud- und Edge-Computing nicht als Gegensatz«

Die Bedrohungen durch Cyber-Kriminelle ändern sich laufend. Wie garantieren Sie Ihren Kunden, dass diese täglich aktuelle Sicherheitsmaßnahmen vorfinden?

Winzenried: Unsere Entwickler sehen es als Herausforderung, Angreifern stets eine Nasenlänge voraus zu sein. Sie werden von Sicherheitsexperten unserer Abteilung Corporate Technology unterstützt, die sich um neue Technologien, beispielsweise Post Quantum Cryptography sowie Kooperationen mit Forschungseinrichtungen und Unternehmen kümmern. Sie nehmen die Sichtweise von Hackern ein und unterstützen unsere Entwickler, unsere Produkte zu härten. Unser Professional Services Team unterstützt unsere Kunden dabei, die Sicherheit ihrer Software zu analysieren und zu verbessern.

Jedoch kommt auch die Praxis nicht zu kurz: Inzwischen haben wir mehrfach mit Wettbewerben die internationale Hackerwelt herausgefordert, allerdings ist es keinem gelungen, die geschützte Wettbewerbssoftware zu knacken. Der letzte Wettbewerb fand 2017 statt. Gemeinsam mit dem Karlsruher Institut für Technologie (KIT) und dem Forschungszentrum Informatik haben wir erfolgreich unsere Blurry-Box-Schutztechnik entwickelt und unter Beweis gestellt. Für die Technik wurden wir mit dem ersten Platz beim Deutschen IT-Sicherheitspreis der Horst-Goertz-Stiftung, dem höchstdotierten IT-Sicherheitspreis in Deutschland, ausgezeichnet.

Hersteller können zwischen verschiedenen Containern, welche die besonderen Anforderungen der Industrie erfüllen, wählen, um ihre Software zu schützen und zu lizenzieren.

https://www.elektroniknet.de/elektronik/embedded/wir-wollen-angreifern-stets-eine-nasenlaenge-voraus-sein-176762.html

Stichwort IoT: Wie stellen Sie eine sichere Verbindung von IoT-Geräten her?
Winzenried: Die wachsende Vernetzung erfordert, dass jedes Gerät und jede Maschine eine fälschungssichere Identität haben. Zur Abwehr von Manipulationen nutzt CodeMeter Zertifikate und digitale Signaturen. Die digitalen Code-Signaturen werden mit dem öffentlichen Schlüssel verifiziert, so wird veränderter oder manipulierter Code sicher erkannt und ausschließlich Code von berechtigten Herausgebern geladen und ausgeführt.

Sie haben bereits Projekte mit dem DFKI und der SmartFactoryKL erfolgreich abgeschlossen. Welche KI-Aktivitäten planen Sie derzeit?
Winzenried: In diesen Projekten haben wir uns sehr früh um die Themen Lizenzierung in der Cloud auf der einen Seite, genauso wie die Implementierung von Security in vernetzten Produktionssystemen mit CodeMeter und OPC UA auf der anderen Seite gekümmert. Heute arbeitet unsere Corporate Technology an KI-Verfahren für den automatischen Schutz von Software und mit unserer Entwicklung an Anwendungen zum Schutz der KI-Algorithmen unserer Kunden mit speziellen Schutzverfahren für Software in Python.

Im Embedded-Bereich stellt sich derzeit oft die Frage nach Cloud- vs. Edge-Computing. Welche Technik sehen Sie als sicherer und warum?
Winzenried: Wir sehen Cloud- und Edge-Computing nicht als Gegensatz. Edge Computing wird benötigt, um die Datenmenge in den Griff zu bekommen und die Verfügbarkeit des Gesamtsystems zu erhöhen. CodeMeter deckt als skalierbares Produkt den Schutz von Anwendungen auf Edge-Computern ebenso wie in der Cloud ab. Hersteller können flexibel unterschiedliche Containerarten als Schlüsselspeicher einsetzen: den hardwarebasierten »CmDongle«, auch als Chip, die softwarebasierte »CmActLicense« oder den cloudbasierten »CmCloudContainer«. Besonders geeignet für den Einsatz in der Cloud sind CmActLicenses und CmCloudContainer, etwa für Software in der Microsoft Azure-Cloud. Für Edge-Computing und On-Premises können Anwender CmDongles, CmActLicense und CmCloudContainer gleichermaßen nutzen.

Vielen Dank für das Gespräch.

© Wibu-Systems

Oliver Winzenried studierte Elektrotechnik an der Universität Karlsruhe und gründete 1989 mit Marcellus Buchheit das Unternehmen Wibu-Systems, dessen

https://www.elektroniknet.de/elektronik/embedded/wir-wollen-angreifern-stets-eine-nasenlaenge-voraus-sein-176762.html

Vorstand er heute ist. Seine Leidenschaft für Schutz von Software findet sich in diversen Patenten und Produkten, beispielsweise Dongles. Sein umfassendes Know-How stellt er Vereinen wie dem VDMA und dem Bitkom zur Verfügung.